MN

Notice of Allowability	**Application No.** 10/653,500	**Applicant(s)** MIZRAH, LEN L.	
	Examiner Minh Dinh	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *examiner's amendment authorized on 9/12/07*.

2. ☒ The allowed claim(s) is/are *1, 4-10, 13-19, 22-27 and 31*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mark Haynes on 09/12/07.

The claims have been amended as follows:

1. (amended) A method for mutual authentication of a first station and a second station, comprising:

providing a particular data random key at the first station, disassembling and veiling the particular data random key by forming a first conversion array seeded by a shared secret and then encrypting the first conversion array to produce a first encrypted data set, where access to the shared secret indicates authenticity of the first station;

sending a first message to the second station including the first encrypted data set key, where the second station decrypts first encrypted data set and unveils and reassembles said particular data random key using the shared secret, and where the second station disassembles and veils a version of the particular data random key by forming a second conversion array seeded by the shared secret and then encrypts the second conversion array to produce a second encrypted ~~key~~ data set, and sends a second message to the first station carrying the second encrypted data set, where access to the shared secret indicates authenticity of the second station;

receiving the second message, and decrypting the second encrypted data set, and reassembling and unveiling the version of the particular data random key at the first station using the shared secret; ~~and~~

determining at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so providing an additional particular data random key at the first station, disassembling and veiling the additional particular data random key by forming a third conversion array seeded by ~~an additional~~ the shared secret and then encrypting the third conversion array to produce a ~~first additional~~ third encrypted data set, where access to the ~~additional~~ shared secret indicates authenticity of the first station;

sending a third message to the second station including the ~~first additional~~ third encrypted data set, where the second station decrypts the ~~first additional~~ third encrypted data set and reassembles and unveils said additional particular data random key using the ~~additional~~ shared secret, and where the second station disassembles and veils a version of the additional particular data random key by forming a fourth conversion array seeded by the ~~additional-~~shared secret and then encrypts the fourth conversion array to produce a ~~second additional~~ fourth encrypted data set, and sends a fourth message to the first station carrying the ~~second additional~~ fourth encrypted data set, where access to the ~~additional~~ shared secret indicates authenticity of the second station; ~~and~~

receiving the fourth message, and decrypting the ~~second additional~~ fourth encrypted data set and reassembling and unveiling the version of the additional particular data random key at the first station using the shared secret;[[, and]]

determining at the first station if the version of the additional data random key matches an expected version of the additional data random key, and if so ~~continuing with further exchanges of messages with the second station~~ disassembling and veiling the additional particular data random key by forming a fifth conversion array seeded by an additional shared secret and then encrypting the fifth conversion array to produce a fifth encrypted data set, where access to the additional shared secret indicates authenticity of the first station; and

sending a fifth message to the second station including the fifth encrypted data set, where the second station decrypts the fifth encrypted data set, reassembles and unveils said additional particular data random key using the additional shared secret, and determines at the second station if a version of the additional data random key matches an expected version of the additional data random key.

3. (canceled)

10. (amended) A data processing apparatus, comprising:

a processor, a communication interface adapted for connection to a communication medium, and memory storing instructions for execution by the data processor, the instructions including

logic to provide a particular data random key at the first station and to disassemble and veil the particular data random key by forming a first conversion array seeded by a shared secret and then to encrypt the first conversion array to produce a first encrypted data set, where access to the shared secret indicates authenticity of the first station;

logic to send a first message to the second station including the first encrypted data set, where the second station decrypts and unveils the first encrypted data set using the shared secret, and where the second station disassembles and veils a version of the particular data random key by forming a second conversion array seeded by the shared secret and then [[to encrypt]] encrypts the second conversion array to produce a second encrypted data set, and sends a second message to the first station carrying the second encrypted data set, where access to the shared secret indicates authenticity of the second station;

logic to receive the second message, and to decrypt and unveil the version of the particular data random key at the first station using the shared secret; ~~and~~

logic to determine at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so provide an additional particular data random key at the first station, disassemble and veil the additional particular data random key by forming a third conversion array seeded by ~~an additional~~ the shared secret and then to encrypt the third conversion array to produce a ~~first additional~~ third encrypted data set, where access to the ~~additional~~ shared secret indicates authenticity of the first station;

logic to send a third message to the second station including the~~ first additional~~ third encrypted data set, where the second station decrypts the ~~first additional~~ third encrypted data set and reassembles and unveils the additional particular data random key using the ~~additional~~ shared secret, and where the second station disassembles and veils a version of the additional particular data random key by forming a fourth conversion array seeded by the ~~additional~~ shared secret and then encrypts the fourth conversion array to produce a ~~second additional~~ fourth encrypted data set, and sends a fourth message to the first station carrying the ~~second additional~~ fourth encrypted data set, where access to the ~~additional~~ shared secret indicates authenticity of the second station;

logic to receive the fourth message, and decrypt the ~~second additional~~ fourth encrypted data set and to reassemble and unveil the version of the additional particular data random key at the first station using the shared secret;[[, and]]

logic to determine at the first station if the version of the additional data random key matches an expected version of the additional data random key, and if so to ~~continuing with further exchanges of messages with the second station~~ disassemble and veil the additional particular data random key by forming a fifth conversion array seeded by an additional shared secret and then encrypt the fifth conversion array to produce a fifth encrypted data set, where access to the additional shared secret indicates authenticity of the first station; and

logic to send a fifth message to the second station including the fifth encrypted data set, where the second station can decrypt the fifth encrypted data set, and can reassemble and unveil said additional particular data random key using the additional shared secret, in order to determine at the second station if a version of the additional data random key matches an expected version of the additional data random key.

12. (cancel)

19. (amended) An article, comprising:

machine readable data storage medium having computer program instructions stored therein for establishing a communication session on a communication medium between a first data processing station and a second data processing station having access to the communication medium, said instructions comprising

logic to provide a particular data random key at the first station and to disassemble and veil the particular data random key by forming a first conversion array seeded by a shared secret and then to encrypt the first conversion array to produce a first encrypted data set, where access to the shared secret indicates authenticity of the first station;

logic to send a first message to the second station including the first encrypted data set, where the second station decrypts and unveils the first encrypted data set using the shared secret, and where the second station disassembles and veils a version of the particular data random key by forming a second conversion array seeded by the shared secret and then to encrypt the second conversion array to produce a second encrypted data set, and sends a second message to the first station carrying the second encrypted data set, where access to the shared secret indicates authenticity of the second station;

logic to receive the second message, and to decrypt and unveil the version of the particular data random key at the first station using the shared secret; ~~and~~

logic to determine at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so provide an additional particular data random key at the first station, disassemble and veil the additional particular data random key by forming a third conversion array seeded by ~~an additional~~ the shared secret and then to encrypt the third conversion array to produce a ~~first additional~~ third encrypted data set, where access to the ~~additional~~ shared secret indicates authenticity of the first station;

logic to send a third message to the second station including the~~-first additional~~ third encrypted data set, where the second station decrypts the ~~first additional~~ third encrypted data set and reassembles and unveils the additional particular data random key using the ~~additional~~ shared secret, and where the second station disassembles and veils a version of the additional particular data random key by forming a fourth conversion array seeded by the~~-additional~~ shared secret and then encrypts the fourth conversion array to produce a ~~second additional~~ fourth encrypted data set, and sends a fourth message to the first station carrying the ~~second additional~~ fourth encrypted data set, where access to the ~~additional-~~shared secret indicates authenticity of the second station;

logic to receive the fourth message, and decrypt the ~~second additional~~ fourth encrypted data set and to reassemble and unveil the version of the additional particular data random key at the first station using the shared secret;[[, and]]

logic to determine at the first station if the version of the additional data random key matches an expected version of the additional data random key, and if so to ~~continuing with further exchanges of messages with the second station~~ disassemble and veil the additional particular data random key by forming a fifth conversion array seeded by an additional shared secret and then encrypt the fifth conversion array to produce a fifth encrypted data set, where access to the additional shared secret indicates authenticity of the first station; and

logic to send a fifth message to the second station including the fifth encrypted data set, where the second station can decrypt the fifth encrypted data set, and can reassemble and unveil said additional particular data random key using the additional shared secret, in order to determine at the second station if a version of the additional data random key matches an expected version of the additional data random key.

21. (canceled)

28. (cancel)

29. (cancel)

30. (cancel)

31. (amended) A method for mutual authentication of a first station and a second station, comprising:

providing a particular data random key at the first station, disassembling and veiling the particular data random key by forming a first conversion array seeded by a shared secret and then encrypting the first conversion array to produce a first encrypted data set, where access to the shared secret indicates authenticity of the first station;

sending a first message to the second station including the first encrypted data set, where the second station decrypts first encrypted data set and unveils and reassembles said particular data random key using the shared secret;

receiving the first message at the second station and decrypting the first encrypted data set, and reassembling and unveiling the particular data random key at the second station; and determining at the second station if the particular data random key matches an expected version the particular data random key, and if so and disassembling and veiling a version of the particular data random key by forming a second conversion array seeded by the shared secret and then encrypting the second conversion array to produce a second encrypted~~key~~ data set, and sending a second message to the first station carrying the second encrypted data set, where access to the shared secret indicates authenticity of the second station;

receiving the second message at the first station, and decrypting the second encrypted data set, and reassembling and unveiling the version of the particular data random key at the first station using the shared secret; ~~and~~

determining at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so providing an additional particular data random key at the first station, disassembling and veiling the additional particular data random key by forming a third conversion array seeded by ~~an additional~~ the shared secret and then encrypting the third conversion array to produce a ~~first additional~~ third encrypted data set, where access to the ~~additional~~ shared secret indicates authenticity of the first station;

sending a third message to the second station including the ~~first additional~~ third encrypted data set;

receiving the third message at the second station and decrypting the ~~first additional~~ third encrypted data set and unveiling and reassembling the additional particular data random key using the ~~additional~~ shared secret, and determining at the second station if the additional particular data random key matches an expected version the additional particular data random key, and if so disassembling and veiling a version of the additional particular data random key by forming a fourth conversion array seeded by the ~~additional~~ shared secret and then encrypting the fourth conversion array to produce a ~~second additional~~ fourth encrypted data set;

sending a fourth message to the first station carrying the ~~second additional~~ fourth encrypted data set, where access to the ~~additional~~ shared secret indicates authenticity of the second station;

receiving the fourth message, and decrypting the ~~second additional~~ fourth encrypted data set and unveiling and reassembling the version of the additional particular data random key at the first station using the shared secret; ~~and~~

determining at the first station if the version of the additional data random key matches an expected version the additional data random key, and if so ~~continuing with further exchanges of messages with the second station~~ disassembling and veiling the additional particular data random key by forming a fifth conversion array seeded by an additional shared secret and then encrypting the fifth conversion array to produce a fifth encrypted data set, where access to the additional shared secret indicates authenticity of the first station;

sending a fifth message to the second station including the fifth encrypted data set;

receiving the fifth message at the second station, and decrypting the fifth encrypted data set, and unveiling and reassembling said additional particular data random key using the additional shared secret; and

determining at the second station if a version of the additional data random key matches an expected version of the additional data random key.

Election/Restrictions

2. Claims 1, 10 and 19 are allowable. The restriction requirement among species (a), (b) and (c), as set forth in the Office action mailed on 03/29/07, has been reconsidered in view of the allowability of claims to the elected invention pursuant to MPEP § 821.04(a). **The restriction requirement is hereby withdrawn as to any claim that requires all the limitations of an allowable claim**. Claims 5-7, 14-16 and 23-25, directed to species (a), (b) and (c) are no longer withdrawn from consideration because the claims require all the limitations of an allowable claim.

In view of the above noted withdrawal of the restriction requirement, applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application. Once a restriction requirement is withdrawn, the provisions of 35 U.S.C. 121 are no longer applicable. See *In re Ziegler*, 443 F.2d 1211, 1215, 170 USPQ 129, 131-32 (CCPA 1971). See also MPEP § 804.01.

Allowable Subject Matter

3. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method and system for performing mutual authentication between a first station and a second station wherein the first station veils a random key using a first conversion array seeded by a shared secret, encrypts the veiled random key and sends a first message including the encrypted key to the second station; the second station first decrypts and unveils the random key using the shared secret, and then veils a version of the random key using a second conversion array seeded by the shared secret, encrypts the veiled version of the random key and sends a second message including the encrypted veiled version of the random key to the first station; the first station then decrypts and unveils the version of the random key. More specifically, independent claims 1, 10, 19 and 31 identify the uniquely distinct features: performing the same process by the first and

second stations (the same steps in the same order) to an additional random key. The closest prior art include: (a) Bellovin et al. (5,241,599) teaches a method for mutual authentication between a first entity and second entity wherein the first entity encrypts a random value using a shared secret, sends the encrypted random value to the second entity; the second entity decrypts the random value, encrypts a version of the random value using the shared secret and sends the encrypted version of the random data to the first entity, who then decrypts the version of the random data; (b) Nessett et al. (6,920,559) teaches a method for mutual authentication similar to that of Bellovin; and (c) "FIPS 46-3 Data Encryption Standard (DES)" teaches performing multiple DES encryption (i.e., Triple DES) on data, wherein single DES encryption veils (i.e., conceals) data using a conversion array seeded by a shared secret. However, Bellovin, Nessett, and "FIPS 46-3", either alone or in combination, do not teach the specific features mentioned above.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MD/
Minh Dinh
Examiner
Art Unit 2132

09/14/07

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100